6

Attorney's Docket No.: 12732-032001 / US4876

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Shunpei YAMAZAKI et al. Art Unit : Unknown
Serial No. : Not assigned yet Examiner : Unknown
Filed : April 26 2001
Title : A SYSTEM FOR IDENTIFYING AN INDIVIDUAL, A METHOD FOR IDENTIFYING AN INDIVIDUAL OR A BUSINESS METHOD

Commissioner for Patents
Washington, D.C. 20231

TRANSMITTAL OF PRIORITY DOCUMENT UNDER 35 USC §119

Applicant hereby confirms his claim of priority under 35 USC §119 from the following application: Japan Application No. 2000-126513 filed April 26, 2000. A certified copy of each application from which priority is claimed is submitted herewith.

Please apply any charges or credits to Deposit Account No. 06-1050.

Respectfully submitted,

Date: April 26, 2001

William Hare

William D. Hare
Reg. No. 44,739

Fish & Richardson P.C.
601 Thirteenth Street, NW
Washington, DC 20005
Telephone: (202) 783-5070
Facsimile: (202) 783-2331

40053761.doc

日　本　国　特　許　庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　４月２６日

出願番号
Application Number: 特願２０００－１２６５１３

出願人
Applicant (s): 株式会社半導体エネルギー研究所

２００１年　３月　２日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２００１－３０１２５５６

【書類名】　特許願
【整理番号】　P004876
【提出日】　平成12年 4月26日
【あて先】　特許庁長官　殿
【発明者】
　【住所又は居所】　神奈川県厚木市長谷３９８番地　株式会社半導体エネルギー研究所内
　【氏名】　山崎　舜平
【発明者】
　【住所又は居所】　神奈川県厚木市長谷３９８番地　株式会社半導体エネルギー研究所内
　【氏名】　小山　潤
【特許出願人】
　【識別番号】　000153878
　【氏名又は名称】　株式会社半導体エネルギー研究所
　【代表者】　山崎　舜平
【手数料の表示】
　【予納台帳番号】　002543
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
【プルーフの要否】　要

【書類名】明細書

【発明の名称】　本人認証システム

【特許請求の範囲】

【請求項１】

顧客を識別する本人認証システムであって、

前記顧客の生体情報を記憶する手段と、

前記顧客の生体情報を読み取る手段と、

前記読み取った生体情報を前記記憶した生体情報と照合する手段と、

前記照合が合致した場合、サーバーに合致したことを情報として送る手段と、

を有することを特長とする本人認証システム。

【請求項２】

顧客を識別する本人認証システムであって、

前記顧客の複数の生体情報を記憶する手段と、

前記顧客の生体情報を読み取る手段と、

前記読み取った生体情報を前記記憶した複数の生体情報と照合する手段と、

前記読み取った生体情報が、前記記憶した複数の生体情報のうち少なくとも１つと合致した場合、サーバーに合致したことを情報として送る手段と、

を有することを特長とする本人認証システム。

【請求項３】

顧客を識別する本人認証システムであって、

前記顧客の複数の生体情報を記憶する手段と、

前記顧客の複数の生体情報を読み取る手段と、

前記読み取った複数の生体情報を前記記憶した複数の生体情報と照合する手段と、

前記読み取った複数の生体情報のそれぞれが、前記記憶した複数の生体情報のうち少なくとも１つと合致した場合、サーバーに合致したことを情報として送る手段と、

を有することを特長とする本人認証システム。

【請求項４】

顧客を識別する本人認証システムであって、

前記顧客の生体情報を記憶する手段と、

前記顧客の生体情報を読み取る手段と、

前記読み取った生体情報を前記記憶した生体情報と照合する手段と、

前記照合が合致した場合、サーバーに合致したことを情報として、インターネットを介して送る手段と、

を有することを特長とする本人認証システム。

【請求項５】

顧客を識別する本人認証システムであって、

前記顧客の複数の生体情報を記憶する手段と、

前記顧客の生体情報を読み取る手段と、

前記読み取った生体情報を前記記憶した複数の生体情報と照合する手段と、

前記照合の結果、前記読み取った生体情報が、前記記憶した複数の生体情報のうち少なくとも１つと合致した場合、サーバーに前記照合が合致したことを情報として、インターネットを介して送る手段と、

を有することを特長とする本人認証システム。

【請求項６】

顧客を識別する本人認証システムであって、

前記顧客の複数の生体情報を記憶する手段と、

前記顧客の複数の生体情報を読み取る手段と、

前記読み取った複数の生体情報を前記記憶した複数の生体情報と照合する手段と、

前記照合の結果、前記読み取った複数の生体情報のそれぞれが、前記記憶した複数の生体情報のうち少なくとも１つと合致した場合、サーバーに前記照合が合致したことを情報として、インターネットを介して送る手段と、

を有することを特長とする本人認証システム。

【請求項７】

顧客を識別する本人認証システムであって、

前記顧客の生体情報を記憶する手段と、

前記顧客の生体情報を読み取る手段と、

前記読み取った生体情報を前記記憶した生体情報と照合する手段と、

前記照合が合致した場合、サーバーに合致したことを情報として送る手段と、

前記サーバーが前記顧客の取引先に前記照合が合致したことを情報として送る手段と、

を有し、

前記取引先が、前記照合が合致したことを情報として受け取った後に、前記顧客と前記取引先との間で取引が開始されることを特長とする本人認証システム。

【請求項８】

顧客を識別する本人認証システムであって、

前記顧客の複数の生体情報を記憶する手段と、

前記顧客の生体情報を読み取る手段と、

前記読み取った生体情報を前記記憶した複数の生体情報と照合する手段と、

前記照合の結果、前記読み取った生体情報が前記記憶した複数の生体情報のうち少なくとも１つと合致した場合、サーバーに前記照合が合致したことを情報として送る手段と、

前記サーバーが前記顧客の取引先に前記照合が合致したことを情報として送る手段と、

を有し、

前記取引先が、前記照合が合致したことを情報として受け取った後に、前記顧客と前記取引先との間で取引が開始されることを特長とする本人認証システム。

【請求項９】

顧客を識別する本人認証システムであって、

前記顧客の複数の生体情報を記憶する手段と、

前記顧客の複数の生体情報を読み取る手段と、

前記読み取った複数の生体情報を前記記憶した複数の生体情報と照合する手段と、

前記照合の結果、前記読み取った複数の生体情報のそれぞれが、前記記憶した複数の生体情報のうち少なくとも１つと合致した場合、サーバーに前記照合が合

致したことを情報として送る手段と、

前記サーバーが前記顧客の取引先に前記照合が合致したことを情報として送る手段と、

を有し、

前記取引先が、前記照合が合致したことを情報として受け取った後に、前記顧客と前記取引先との間で取引が開始されることを特長とする本人認証システム。

【請求項１０】

顧客を識別する本人認証システムであって、

前記顧客の生体情報を記憶する手段と、

前記顧客の生体情報を読み取る手段と、

前記読み取った生体情報を前記記憶した生体情報と照合する手段と、

前記照合が合致した場合、サーバーに合致したことを情報として送る手段と、

を有し、

前記サーバーに前記照合が合致したことを情報として送った後に、暗証番号を情報として前記サーバーに送り、前記サーバーにおいて記憶されている番号と前記暗証番号が合致した場合、前記記憶された生体情報を書き換えられることを特長とする本人認証システム。

【請求項１１】

顧客を識別する本人認証システムであって、

前記顧客の複数の生体情報を記憶する手段と、

前記顧客の生体情報を読み取る手段と、

前記読み取った生体情報を前記記憶した複数の生体情報と照合する手段と、

前記読み取った生体情報が、前記記憶した複数の生体情報のうち少なくとも１つと合致した場合、サーバーに合致したことを情報として送る手段と、

を有し、

前記サーバーに前記照合が合致したことを情報として送った後に、暗証番号を情報として前記サーバーに送り、前記サーバーにおいて記憶されている番号と前記暗証番号が合致した場合、前記記憶された複数の生体情報を書き換えられることを特長とする本人認証システム。

【請求項１２】

顧客を識別する本人認証システムであって、

前記顧客の複数の生体情報を記憶する手段と、

前記顧客の複数の生体情報を読み取る手段と、

前記読み取った複数の生体情報を前記記憶した複数の生体情報と照合する手段と、

前記読み取った複数の生体情報のそれぞれが、前記記憶した複数の生体情報のうち少なくとも１つと合致した場合、サーバーに合致したことを情報として送る手段と、

を有し、

前記サーバーに前記照合が合致したことを情報として送った後に、暗証番号を情報として前記サーバーに送り、前記サーバーにおいて記憶されている番号と前記暗証番号が合致した場合、前記記憶された複数の生体情報を書き換えられることを特長とする本人認証システム。

【請求項１３】

請求項７乃至請求項９のいずれか１項において、前記顧客と前記取引先との間で行われる取引が前記サーバーに設定された条件を満たす場合のみ、前記顧客の識別を要求することを特長とする本人認証システム。

【請求項１４】

請求項１、請求項４、請求項７、請求項１０または請求項１３のいずれか１項に記載の前記生体情報とは、指紋、掌紋または声紋であることを特長とする本人認証システム。

【請求項１５】

請求項２、請求項３、請求項５、請求項６、請求項８、請求項９、請求項１１、請求項１２または請求項１３のいずれか１項に記載の前記複数の生体情報とは、指紋、掌紋または声紋であることを特長とする本人認証システム。

【請求項１６】

請求項１４または請求項１５において、前記掌紋は手ひらの全体の掌紋、もしくは前記手のひらの一部の掌紋であることを特徴とした本人認証システム。

【請求項１７】

請求項１乃至請求項１６のいずれか１項において、前記記憶する手段とは、フラッシュメモリを含むことを特長とする本人認証システム。

【請求項１８】

請求項１乃至請求項１６のいずれか１項において、前記読み取る手段とは、フォトダイオードまたはＣＣＤを含むことを特長とする本人認証システム。

【請求項１９】

請求項１乃至請求項１８のいずれか１項において、

携帯情報端末を用いることを特長とする本人認証システム。

【請求項２０】

請求項１乃至請求項１８のいずれか１項において、

携帯電話を用いることを特長とする本人認証システム。

【請求項２１】

請求項１乃至請求項１８のいずれか１項において、

パーソナルコンピューターを用いることを特長とする本人認証システム。

【００００】

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は本人認証システムに関し、特に、生体情報を用いて本人認証を行うことを特徴とした本人認証システムである。

【０００２】

【従来の技術】

近年、携帯電話、パソコン、携帯情報端末などの通信装置を使用してインターネットに接続する通信技術が急速に発展しつつある。企業、家庭でのインターネット等への接続は、据え置き型のパソコンに電話回線を接続することで行われている。特に近年では、インターネットが簡単に出来るiモードなどの携帯電話が普及し、さまざまな情報交換が簡便に行われるようになった。

【０００３】

通信装置を用いて、インターネット上で金銭授受などの取引を行う場合、本人であることの確認（本人認証作業）が必要である。本人認証作業は、あらかじめ相手先に登録されている暗証番号を、使用者が通信装置により相手先に送信し、相手先で該暗証番号を照合することで行われている。

【０００４】

図１１に従来の本人認証のフローを示す。使用者はまずインターネットに接続し、取引の相手先の指定した条件下で、認証のための数値を通信装置を用いて相手先に送信する。認証のための数値のデータを受信した相手先は、自分のところにあらかじめ登録された暗証番号と、使用者から送られてきた数値との照合を行い、合致するかどうかを確認する。ここで合致が見られれば、使用者は本人と確認され、要望する対応を得ることができる。

【０００５】

【発明が解決しようとする課題】

上記したような従来の通信装置を用いた認証システムでは以下の問題があった。

１、暗証番号が本人以外の人間に漏洩した場合、使用者（顧客）以外に悪用される可能性があり、本人であることの確認が難しい。

２、本人認証作業の際、使用者から相手先へ暗証番号のデータを送信したり、相手先（サーバー）から使用者へ認証の是非をデータとして送信したりするため、通信するのに必要なコストが上昇する。そして使用者と相手先の間においてデータをやりとりする回数が多いため、何らかのエラーにより通信が断絶すると本人認証作業を最初から再び行う必要が生じ、作業が繁雑である。

３、使用者が暗証番号を忘れることで、相手先に再び暗証番号を登録するする必要が生じる。

４、暗証番号を通信機器に入力する際、操作キーの入力に手間がかかる。

【０００６】

本発明は、上記問題を解決することを課題とする。

【０００７】

【課題を解決するための手段】

本発明では本人認証作業を通信装置のみを用いて行い、本人かどうかの確認は、通信装置において使用者の生体情報を照合することで行う。本明細書において生体情報とは、人間が生まれつき持っている身体的な特徴で、なおかつ人間の個体識別が可能な情報を意味し、指紋、掌紋、声紋等が挙げられる。通信装置に使用者の生体情報を入力することで本人認証作業を行い、認証された場合にのみ、相手先に認証されたことを通知する。

【０００８】

相手先に本人だと認証されたら、相手先との取引が開始される。または、相手先が第３者である取引先に認証結果を送信し、使用者と第３者とが取引を開始しても良い。

【０００９】

上記本人認証作業において、使用者の生体情報が通信装置に記憶されている生体情報と合致しない場合、再び使用者の生体情報を通信装置に入力し直すことができる。通信装置に繰り返し生体情報を入力して照合を行おうとしたとき、連続してｎ回以上（ｎは自然数）合致しない場合は相手先に自動的にｎ回以上合致しなかったことを通知するようにしても良い。

【００１０】

また、通信装置に記憶されている使用者の生体情報は複数あっても良く、例えば、指紋と声紋の両方を通信装置に入力することで本人認証作業を行う構成にしても良い。そして通信装置に記憶されている使用者の生体情報を書き換える場合、一度通信装置を用いて本人認証作業を行った後、相手先に生体情報を書き換える際に必要な暗証番号を情報として送り、相手先において暗証番号が合致したら、通信装置に記憶されている生体情報を書き換えることができるようにしても良い。

【００１１】

また生体情報の通信装置への入力は、ＣＣＤやフォトダイオードを用いたラインセンサーやエリアセンサー、マイク等によって行われる。

【００１２】

上記構成によって、暗証番号が本人以外の人間に漏洩して使用者以外に悪用さ

れる可能性が低減する。そして、本人認証作業の際に、使用者と相手先との間においてデータをやりとりする必要がなくなるため、相手先との通信に必要なコストを抑えることができ、何らかのエラーにより通信が断絶し本人認証作業を最初から再び行うという繁雑さを回避することができる。さらに、使用者の生体情報を用いて認証を行うため、使用者が暗証番号を忘れて相手先に再び暗証番号を登録する必要がなくなる。また、暗証番号を通信機器に入力する手間を省くことができる。

【００１３】

以下に本発明の構成を示す。

【００１４】

本発明は、

顧客を識別する本人認証システムであって、

前記顧客の生体情報を記憶する手段と、

前記顧客の生体情報を読み取る手段と、

前記読み取った生体情報を前記記憶した生体情報と照合する手段と、

前記照合が合致した場合、サーバーに合致したことを情報として送る手段と、

を有することを特長とする。

【００１５】

本発明は、

顧客を識別する本人認証システムであって、

前記顧客の複数の生体情報を記憶する手段と、

前記顧客の生体情報を読み取る手段と、

前記読み取った生体情報を前記記憶した複数の生体情報と照合する手段と、

前記読み取った生体情報が、前記記憶した複数の生体情報のうち少なくとも１つと合致した場合、サーバーに合致したことを情報として送る手段と、

を有することを特長とする。

【００１６】

本発明は、

顧客を識別する本人認証システムであって、

前記顧客の複数の生体情報を記憶する手段と、

前記顧客の複数の生体情報を読み取る手段と、

前記読み取った複数の生体情報を前記記憶した複数の生体情報と照合する手段と、

前記読み取った複数の生体情報のそれぞれが、前記記憶した複数の生体情報のうち少なくとも１つと合致した場合、サーバーに合致したことを情報として送る手段と、

を有することを特長とする。

【００１７】

本発明は、

顧客を識別する本人認証システムであって、

前記顧客の生体情報を記憶する手段と、

前記顧客の生体情報を読み取る手段と、

前記読み取った生体情報を前記記憶した生体情報と照合する手段と、

前記照合が合致した場合、サーバーに合致したことを情報として、インターネットを介して送る手段と、

を有することを特長とする。

【００１８】

本発明は、

顧客を識別する本人認証システムであって、

前記顧客の複数の生体情報を記憶する手段と、

前記顧客の生体情報を読み取る手段と、

前記読み取った生体情報を前記記憶した複数の生体情報と照合する手段と、

前記照合の結果、前記読み取った生体情報が、前記記憶した複数の生体情報のうち少なくとも１つと合致した場合、サーバーに前記照合が合致したことを情報として、インターネットを介して送る手段と、

を有することを特長とする。

【００１９】

本発明は、

顧客を識別する本人認証システムであって、

前記顧客の複数の生体情報を記憶する手段と、

前記顧客の複数の生体情報を読み取る手段と、

前記読み取った複数の生体情報を前記記憶した複数の生体情報と照合する手段と、

前記照合の結果、前記読み取った複数の生体情報のそれぞれが、前記記憶した複数の生体情報のうち少なくとも１つと合致した場合、サーバーに前記照合が合致したことを情報として、インターネットを介して送る手段と、

を有することを特長とする。

【００２０】

本発明は、

顧客を識別する本人認証システムであって、

前記顧客の生体情報を記憶する手段と、

前記顧客の生体情報を読み取る手段と、

前記読み取った生体情報を前記記憶した生体情報と照合する手段と、

前記照合が合致した場合、サーバーに合致したことを情報として送る手段と、

前記サーバーが前記顧客の取引先に前記照合が合致したことを情報として送る手段と、

を有し、

前記取引先が、前記照合が合致したことを情報として受け取った後に、前記顧客と前記取引先との間で取引が開始されることを特長とする。

【００２１】

本発明は、

顧客を識別する本人認証システムであって、

前記顧客の複数の生体情報を記憶する手段と、

前記顧客の生体情報を読み取る手段と、

前記読み取った生体情報を前記記憶した複数の生体情報と照合する手段と、

前記照合の結果、前記読み取った生体情報が前記記憶した複数の生体情報のうち少なくとも１つと合致した場合、サーバーに前記照合が合致したことを情報と

して送る手段と、

前記サーバーが前記顧客の取引先に前記照合が合致したことを情報として送る手段と、

を有し、

前記取引先が、前記照合が合致したことを情報として受け取った後に、前記顧客と前記取引先との間で取引が開始されることを特長とする。

【００２２】

本発明は、

顧客を識別する本人認証システムであって、

前記顧客の複数の生体情報を記憶する手段と、

前記顧客の複数の生体情報を読み取る手段と、

前記読み取った複数の生体情報を前記記憶した複数の生体情報と照合する手段と、

前記照合の結果、前記読み取った複数の生体情報のそれぞれが、前記記憶した複数の生体情報のうち少なくとも１つと合致した場合、サーバーに前記照合が合致したことを情報として送る手段と、

前記サーバーが前記顧客の取引先に前記照合が合致したことを情報として送る手段と、

を有し、

前記取引先が、前記照合が合致したことを情報として受け取った後に、前記顧客と前記取引先との間で取引が開始されることを特長とする。

【００２３】

本発明は、

顧客を識別する本人認証システムであって、

前記顧客の生体情報を記憶する手段と、

前記顧客の生体情報を読み取る手段と、

前記読み取った生体情報を前記記憶した生体情報と照合する手段と、

前記照合が合致した場合、サーバーに合致したことを情報として送る手段と、

を有し、

前記サーバーに前記照合が合致したことを情報として送った後に、暗証番号を情報として前記サーバーに送り、前記サーバーにおいて記憶されている番号と前記暗証番号が合致した場合、前記記憶された生体情報を書き換えられることを特長とする。

【００２４】

本発明は、

顧客を識別する本人認証システムであって、

前記顧客の複数の生体情報を記憶する手段と、

前記顧客の生体情報を読み取る手段と、

前記読み取った生体情報を前記記憶した複数の生体情報と照合する手段と、

前記読み取った生体情報が、前記記憶した複数の生体情報のうち少なくとも１つと合致した場合、サーバーに合致したことを情報として送る手段と、

を有し、

前記サーバーに前記照合が合致したことを情報として送った後に、暗証番号を情報として前記サーバーに送り、前記サーバーにおいて記憶されている番号と前記暗証番号が合致した場合、前記記憶された複数の生体情報を書き換えられることを特長とする。

【００２５】

本発明は、

顧客を識別する本人認証システムであって、

前記顧客の複数の生体情報を記憶する手段と、

前記顧客の複数の生体情報を読み取る手段と、

前記読み取った複数の生体情報を前記記憶した複数の生体情報と照合する手段と、

前記読み取った複数の生体情報のそれぞれが、前記記憶した複数の生体情報のうち少なくとも１つと合致した場合、サーバーに合致したことを情報として送る手段と、

を有し、

前記サーバーに前記照合が合致したことを情報として送った後に、暗証番号を

情報として前記サーバーに送り、前記サーバーにおいて記憶されている番号と前記暗証番号が合致した場合、前記記憶された複数の生体情報を書き換えられることを特長とする。

【００２６】

本発明は、前記顧客と前記取引先との間で行われる取引が前記サーバーに設定された条件を満たす場合のみ、前記顧客の識別を要求することを特長としていても良い。

【００２７】

前記生体情報とは、指紋、掌紋または声紋であることを特長としていても良い。

【００２８】

前記掌紋は手ひらの全体の掌紋、もしくは前記手のひらの一部の掌紋であることを特徴としていても良い。

【００２９】

前記顧客の生体情報を記憶する手段とは、フラッシュメモリであることを特長としていても良い。

【００３０】

前記顧客の生体情報を読み取る手段とは、フォトダイオードまたはＣＣＤであることを特長としていても良い。

【００３１】

本発明は、携帯情報端末、携帯電話またはパーソナルコンピューターを用いることを特長としていても良い。

【００３２】

【発明の実施の形態】

図１に本発明の本人認証システムのフローを示す。まず通信装置の操作キーを操作し、生体情報を収集する。あらかじめプログラムされていれば、１つの操作キーを押すことによって生体情報の収集が開始されるようにすることも可能である。また、通信装置の電源投入時に自動的に生体情報収集がはじめられるようにすることも可能である。

【００３３】

得られた生体情報は、あらかじめ通信装置の中の不揮発性メモリなどで形成されている内蔵メモリに蓄えられている本人の生体情報（内蔵メモリデータ）と比較される。ここで、２つの生体情報が合致すると判断されれば、使用者は通信装置の正しい所有者であると認証される。認証終了後、認証済であるという情報を有するデータを相手先に送信する。このとき、認証作業はすでに終了しているので、新たに相手先との間で認証作業をする必要はなく、通信装置から認証は終了しているという情報を相手先は受け取るだけでよい。

【００３４】

本実施の形態の本人認証システムに使用する通信装置はセンサーまたはマイクを内蔵している。ここで用いるセンサーはラインセンサーまたはエリアセンサーであり、使用者の生態情報を読み取るのに使用する。

【００３５】

次に、本発明の本人認証システムに用いられる生体情報のうち、指紋及び掌紋について説明する。

【００３６】

図２に人間の右手を示す。生体情報として通信装置に読み取られるのは、手のひらの一部である掌紋１、手のひら全体である掌紋２、親指の指紋、人差し指の指紋、中指の指紋、薬指の指紋または小指の指紋である。上記生体情報のうち、１つの生体情報だけを通信機器に記憶させても良いし、複数の生体情報を記憶させても良い。

【００３７】

手のひらの一部である掌紋１、手のひら全体である掌紋２、親指の指紋、人差し指の指紋、中指の指紋、薬指の指紋及び小指の指紋は、個々の人間に特有のものであるため、第３者による通信装置の悪用を防ぐことができる。

【００３８】

本人認証作業が終了し、相手先が認証終了の情報を通信装置から受け取ると、使用者と相手先との間で取引が開始される。または、相手先が第３者である取引先に認証結果を送信し、使用者と第３者である取引先とが取引を開始しても良い

【００３９】

図３に使用者と第３者である取引先とが取引する場合のフローを示す。まず使用者が通信装置を用いて本人認証作業を終了したら、通信装置から相手先（サーバー）に本人認証作業が終了したという情報が送信される。

【００４０】

サーバーは、本人認証作業が終了したという情報を受け取ったら、第３者としての取引先に、本人認証済であるという情報を送信する。本人認証済であるという情報を受け取った取引先は、直接使用者と取引を開始する。

【００４１】

上記構成によって、暗証番号が本人以外の人間に漏洩して使用者以外に悪用される可能性が低減する。そして、本人認証作業の際に、使用者と相手先との間においてデータをやりとりする必要がなくなるため、相手先との通信に必要なコストを抑えることができ、何らかのエラーにより通信が断絶し本人認証作業を最初から再び行うという繁雑さを回避することができる。さらに、使用者の生体情報を用いて認証を行うため、使用者が暗証番号を忘れて相手先に再び暗証番号を登録する必要がなくなる。また、暗証番号を通信機器に入力する手間を省くことができる。

【００４２】

【実施例】

以下に、本発明の実施例について説明する。

【００４３】

（実施例１）

以下に本発明において用いられる通信装置の構成と、その動作について説明する。

【００４４】

図４は本実施例の通信装置のブロック図である。この通信装置はアンテナ６０１、送信受信回路６０２、信号を圧縮伸張化、符号化する信号処理回路６０３、制御用マイコン６０４、フラッシュメモリ６０５、操作キー６０６などを有して

いる。そしてされに、センサー６１１、照合回路部６１２などを有している。

【００４５】

操作キー６０６を操作することによって、制御用マイコン６０４がセンサー６１１を制御し、使用者の生体情報を読み取らせる。なお本実施例では、生体情報として、掌紋または指紋を用いる例について説明する。センサー６１１で読み取った使用者の生体情報は、照合回路部６１２に入力される。

【００４６】

照合回路部６１２に入力された使用者の生体情報は、Ａ／Ｄコンバータ６１３においてデジタル信号に変換される。デジタル信号に変換された使用者の生体情報は、ＤＳＰ（デジタルシグナルプロセッサ）６１４に入力され、信号処理される。信号処理とは具体的には、生体情報をより判別しやすくするため、微分フィルタなどを用い映像の濃淡が変わるところを際立たせることである。得られた生体情報はＤＳＰ６１４内部で数値化され、比較回路６１５に入力される。

【００４７】

比較回路６１５はフラッシュメモリ６０５に記憶されている基準となる使用者の生体情報と、ＤＳＰ６１４内部で数値化され比較回路６１５に入力された生体情報とを比較照合する。

【００４８】

生体情報を照合する方法としては、基準となる生体情報と収集した生体情報のそれぞれの特徴を比較して照合する特徴照合方式と、該二つの生体情報を直接比較する画像マッチング方式があるが、どちらの方式を用いても良い。また基準データは１つだけではなく、手の向きを多少変えるなどして、複数の認証データを備えたほうがより確実な認証が可能となる。

【００４９】

ここで合致が見られれば、制御用マイコン６０４は認証信号を出力し、該認証信号は、信号処理回路６０３、送受信回路６０２、アンテナ６０１を介して通信装置から出力される。通信装置から出力された認証信号は、インターネットなどを通じて伝達される。なお、通信装置から出力された認証信号を、インターネットを介さず直接相手先に送信しても良い。

【００５０】

（実施例２）

以下に本発明において用いられる通信装置の構成と、その動作の、実施例１とは異なる例について説明する。

【００５１】

図５は本実施例の通信装置のブロック図である。この通信装置はアンテナ５０１、送信受信回路５０２、信号を圧縮伸張化、符号化する信号処理回路５０３、制御用マイコン５０４、フラッシュメモリ５０５、操作キー５０６などを有している。そしてされに、マイク５１１、アンプ５１６、照合回路部５１２などを有している。

【００５２】

操作キー５０６を操作することによって、制御用マイコン５０４がマイク５１１を制御し、使用者の生体情報を読み取らせる。なお本実施例では、生体情報として、声紋を用いる例について説明する。マイク５１１で読み取った使用者の生体情報は、アンプ５１６によって増幅され、照合回路部５１２に入力される。

【００５３】

照合回路部５１２に入力された使用者の生体情報は、Ａ／Ｄコンバータ５１３においてデジタル信号に変換される。デジタル信号に変換された使用者の生体情報は、ＤＳＰ（デジタルシグナルプロセッサ）５１４に入力され、信号処理される。信号処理とは具体的には、生体情報をより判別しやすくするため、帯域フィルタなどを用い、周波数ごとの音の強さを数値化することである。ＤＳＰ５１４により数値化された生体情報は比較回路５１５に入力される。

【００５４】

比較回路５１５はフラッシュメモリ５０５に記憶されている基準となる使用者の生体情報と、ＤＳＰ５１４内部で数値化され比較回路５１５に入力された生体情報とを比較照合する。

【００５５】

生体情報を照合する方法としては、基準となる生体情報と収集した生体情報のそれぞれの特徴を比較して照合する特徴照合方式と、該二つの生体情報が有する

スペクトルを直接比較する画像マッチング方式があるが、どちらの方式を用いても良い。また基準データは１つだけではなく、発音を多少変えるなどして、複数の認証データを備えたほうがより確実な認証が可能となる。

【００５６】

ここで合致が見られれば、制御用マイコン５０４は認証信号を出力し、該認証信号は、信号処理回路５０３、送受信回路５０２、アンテナ５０１を介して通信装置から出力される。通信装置から出力された認証信号は、インターネットなどを通じて伝達される。なお、通信装置から出力された認証信号を、インターネットを介さず直接相手先に送信しても良い。

【００５７】

本実施例の構成は、実施例１と自由に組み合わせて実施することが可能である。

【００５８】

（実施例３）

次に本発明で用いられる通信装置の１つである、携帯情報端末について述べる。図６に示すのは本実施例の携帯情報端末であり、２７０１は表示用パネル、２７０２は操作用パネルである。表示用パネル２７０１と操作用パネル２７０２は接続部２７０３において接続されている。そして接続部２７０３における、表示用パネル２７０１のセンサー内蔵ディスプレイ２７０４が設けられている面と操作用パネル２７０２の音声入力部２７０８が設けられている面との角度θは、任意に変えることができる。

【００５９】

表示用パネル２７０１はセンサー内蔵ディスプレイ２７０４を有している。センサー内蔵ディスプレイ２７０４はセンサーとしての機能する他に、ディスプレイとしても機能し、画像を表示することが可能である。本実施例ではセンサー内蔵ディスプレイ２７０４にはＥＬディスプレイが用いられている。

【００６０】

また図６に示した携帯情報端末は電話としての機能を有しており、表示用パネル２７０１は音声出力部２７０５を有しており、音声が音声出力部２７０５から

出力される。

【００６１】

操作用パネル２７０２は操作キー２７０６、電源スイッチ２７０７、音声入力部２７０８を有している。なお図６では操作キー２７０６と電源スイッチ２７０７とを別個に設けたが、操作キー２７０６の中に電源スイッチ２７０７が含まれる構成にしても良い。音声入力部２７０８において、音声が入力される。

【００６２】

なお図６では表示用パネル２７０１が音声出力部２７０５を有し、操作用パネル２７０２が音声入力部２７０８を有しているが、本実施例はこの構成に限定されない。表示用パネル２７０１が音声入力部２７０８を有し、操作用パネルが音声出力部２７０５を有していても良い。また音声出力部２７０５と音声入力部２７０８とが共に表示用パネル２７０１に設けられていても良いし、音声出力部２７０５と音声入力部２７０８とが共に操作用パネル２７０２に設けられていても良い。

【００６３】

図７、図８を用いて、図６で示した携帯情報端末の使用方法について説明する。図７に示すように、図６で示した携帯情報端末によって認証を行う場合には、手のひらをセンサー内蔵ディスプレイ２７０４に覆いかぶせるようにして使用する。認証は操作キー２７０６でキー操作を行うとともに、使用者の手相をセンサー内蔵ディスプレイ２７０４が読み取り、認証作業を行う。

【００６４】

なお図７では操作キー２７０６を人差し指で操作している例について示したが、図８に示すように、親指で操作キー２７０６を操作することも可能である。なお操作キー２７０６は操作用パネル２７０２の側面に設けても良い。操作は片手（きき手）の人差し指のみ、または親指のみでも可能である。

【００６５】

以下に図６に示した携帯情報端末の構成と、その動作について説明する。

【００６６】

図９は本実施例の携帯情報端末のブロック図である。この携帯情報端末はアン

テナ９０１、送信受信回路９０２、信号を圧縮伸張化、符号化する信号処理回路９０３、制御用マイコン９０４、フラッシュメモリ９０５、操作キー９０６、音声入力回路９０７、音声出力回路９０８、マイク９０９、スピーカ９１０などを有している。そしてされに、センサー９１１、照合回路部９１２などを有している。

【００６７】

音声入力部２７０８から入力された音声は、マイク９０９に入力され、アナログ信号として音声入力回路９０７に入力される。音声入力回路９０７に入力されたアナログ信号は増幅された後デジタル信号に変換され、信号処理部９０３に入力される。信号処理部９０３において圧縮伸張化、符号化されたデジタル信号は、送受信回路９０２において周波数を変えられて、場合によっては増幅されて、アンテナ９０１から送信される。

【００６８】

またアンテナ９０１において受信した音声情報を有するデジタル信号は、送受信回路９０２において周波数を変えられて、場合によっては増幅されて、信号処理部９０３に入力される。信号処理部９０３に入力されたデジタル信号は圧縮伸張化、符号化され、音声出力回路９０８に入力される。音声出力回路９０８に入力されたデジタル信号はアナログ信号に変換された後増幅され、スピーカー９１０から出力され、音声出力部２７０８から音声として使用者の耳に入力する。

【００６９】

操作キー９０６を操作することによって、制御用マイコン９０４がセンサー９１１を制御し、使用者の生体情報を読み取らせる。なお本実施例では、生体情報として、掌紋または指紋を用いる例について説明する。センサー９１１で読み取った使用者の生体情報は、照合回路部９１２に入力される。

【００７０】

照合回路部９１２に入力された使用者の生体情報は、Ａ／Ｄコンバータ９１３においてデジタル信号に変換される。デジタル信号に変換された使用者の生体情報は、ＤＳＰ（デジタルシグナルプロセッサ）９１４に入力され、信号処理される。信号処理とは具体的には、生体情報をより判別しやすくするため、微分フィ

ルタなどを用い映像の濃淡が変わるところを際立たせることである。得られた生体情報はＤＳＰ９１４内部で数値化され、比較回路９１５に入力される。

【００７１】

比較回路９１５はフラッシュメモリ９０５に記憶されている基準となる使用者の生体情報と、ＤＳＰ９１４内部で数値化され比較回路９１５に入力された生体情報とを比較照合する。

【００７２】

生体情報を照合する方法としては、基準となる生体情報と収集した生体情報のそれぞれの特徴を比較して照合する特徴照合方式と、該二つの生体情報を直接比較する画像マッチング方式があるが、どちらの方式を用いても良い。また基準データは１つだけではなく、手の向きを多少変えるなどして、複数の認証データを備えたほうがより確実な認証が可能となる。

【００７３】

ここで合致が見られれば、制御用マイコン９０４は認証信号を出力し、該認証信号は、信号処理回路９０３、送受信回路９０２、アンテナ９０１を介して携帯情報端末から出力される。携帯情報端末から出力された認証信号は、インターネットなどを通じて伝達される。なお、携帯情報端末から出力された認証信号を、インターネットを介さず直接相手先に送信しても良い。

【００７４】

なお本発明で用いられる通信装置は、本実施例で示した構成の携帯情報端末に限定されない。また本実施例で示した携帯情報端末は、指紋または掌紋を生体情報として利用しているが、声紋を生体情報として利用する構成を有していても良い。

【００７５】

なお、本実施例は、実施例１または２と自由に組み合わせて実施することが可能である。

【００７６】

（実施例４）

本実施例は本発明を使用する状況を述べるものである。本人認証が生体情報ま

での高度な認証が不要な場合は本発明を使用しないこともありえる。小額の金銭移動などの場合は必ずしも必要ではない。

【００７７】

このため、認証の有無が選択できること、たとえば金銭が高額な移動が伴う場合のみに選択的に認証が出来るようにすることも可能である。取引先の状況に合わせ使用することや、あらかじめ携帯情報装置の制御マイコン上に判定基準を設定しておき、数値が一定値を超えた場合のみ使用することが可能である。また、認証結果を必要な場合のみ認証結果をインターネットで伝達することも可能である。

【００７８】

なお、本実施例は、実施例１～実施例３と自由に組み合わせて実施することが可能である。

【００７９】

（実施例５）

本発明に用いられる通信装置として、様々な電子機器を用いることができる。

【００８０】

図１０（Ａ）はパーソナルコンピューター（パソコン）であり、本体２５０１、筐体２５０２、表示部２５０３、キーボード２５０４、センサー２５０５等を含む。本発明では、センサー２５０５を用い、パーソナルコンピューター内に生体情報を取り込むことができる。

【００８１】

なお本実施例では、指紋または掌紋を生体情報として利用する例について示したが、音声入力部を設けて声紋を生体情報として利用する構成にしても良い。またセンサー２５０５と音声入力部を両方設けて、指紋または掌紋と、声紋とを共に利用する構成にしても良い。

【００８２】

図１０（Ｂ）は携帯電話であり、本体２６０１、音声出力部２６０２、音声入力部２６０３、表示部２６０４、操作キー２６０５、アンテナ２６０６を含んでいる。通常の電話をかける場合は表示部２６０４に相手先の電話番号や、電波の

受信状態などが表示される。また、インターネットを使用する場合には、相手先の必要情報が表示されることになる。そして表示部２６０４はセンサーとしても機能し、表示部２６０４において生体情報を取り込むことが可能である。

【００８３】

また、図１０（Ｂ）に示した携帯電話は、表示部２６０４がセンサーとしての機能とディスプレイとしての機能を併せ持っていたが、表示部２６０４をディスプレイとしてのみ利用し、センサーを別個に設ける構成にしても良い。

【００８４】

なお本発明で用いられる通信装置は本実施例で示した電子機器に限定されない。生体情報を取り込み、該生体情報をあらかじめ記憶されている生体情報と照合し、照合が合致したら相手先に認証が終了したことを知らせる機能を有していればよい。

【００８５】

【発明の効果】

本発明の本人認証システムは、暗証番号が本人以外の人間に漏洩して使用者以外に悪用される可能性が低減する。そして、本人認証作業の際に、使用者と相手先との間においてデータをやりとりする必要がなくなるため、相手先との通信に必要なコストを抑えることができ、何らかのエラーにより通信が断絶し本人認証作業を最初から再び行うという繁雑さを回避することができる。さらに、使用者の生体情報を用いて認証を行うため、使用者が暗証番号を忘れて相手先に再び暗証番号を登録する必要がなくなる。また、暗証番号を通信機器に入力する手間を省くことができる。

【図面の簡単な説明】

【図１】　本発明の本人認証システムのフロー。

【図２】　読み取る掌紋または指紋の位置を示す図。

【図３】　使用者とサーバーと第３者としての取引先の関係を示した図。

【図４】　通信装置の構造を示すブロック図。

【図５】　通信装置の構造を示すブロック図。

【図６】　通信装置の一例である携帯情報端末の外観図。

【図７】　通信装置の一例である携帯情報端末の使用例。

【図８】　通信装置の一例である携帯情報端末の使用例。

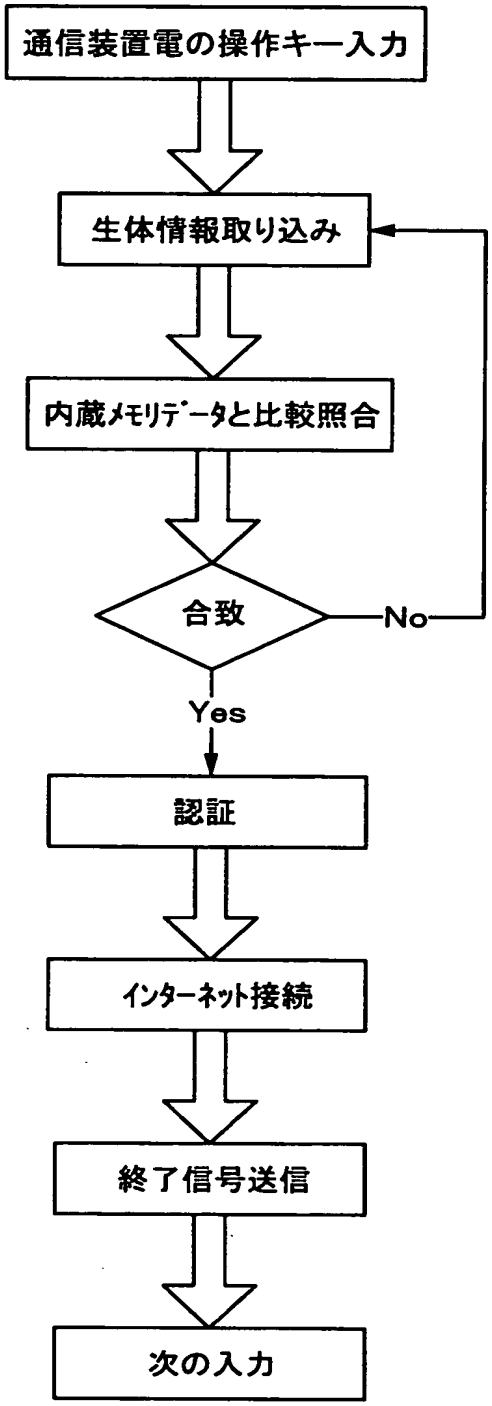
【図９】　通信装置の一例である携帯情報端末の構造を示すブロック図。

【図１０】　通信装置の一例である電子機器の図。

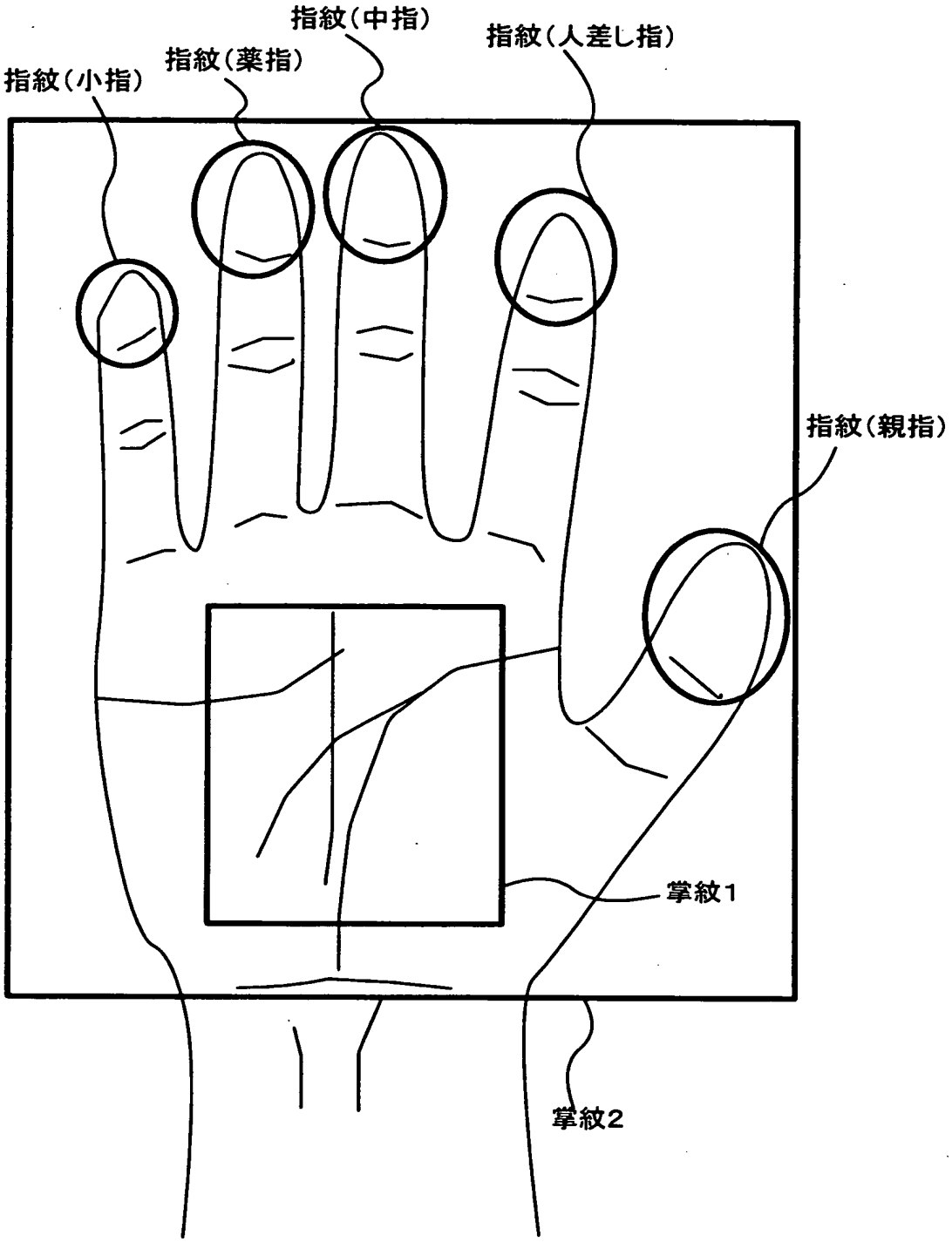
【図１１】　従来の本人認証のフロー。

【書類名】　　図面

【図１】

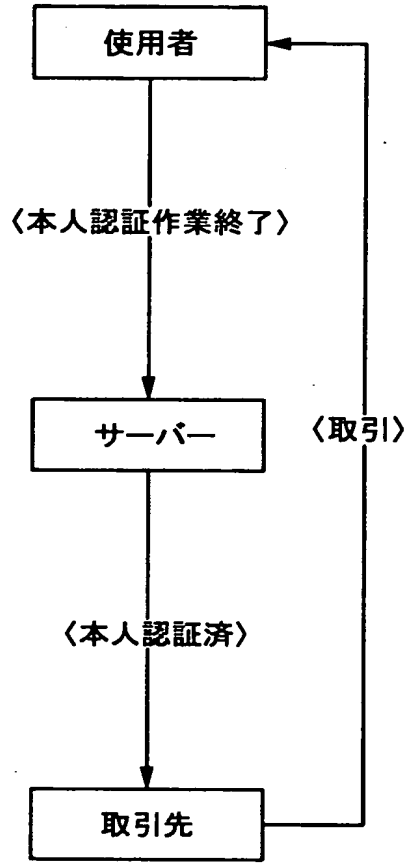

通信装置電の操作キー入力
生体情報取り込み
内蔵ﾒﾓﾘﾃﾞｰﾀと比較照合
合致
No
Yes
認証
インターネット接続
終了信号送信
次の入力

【図２】

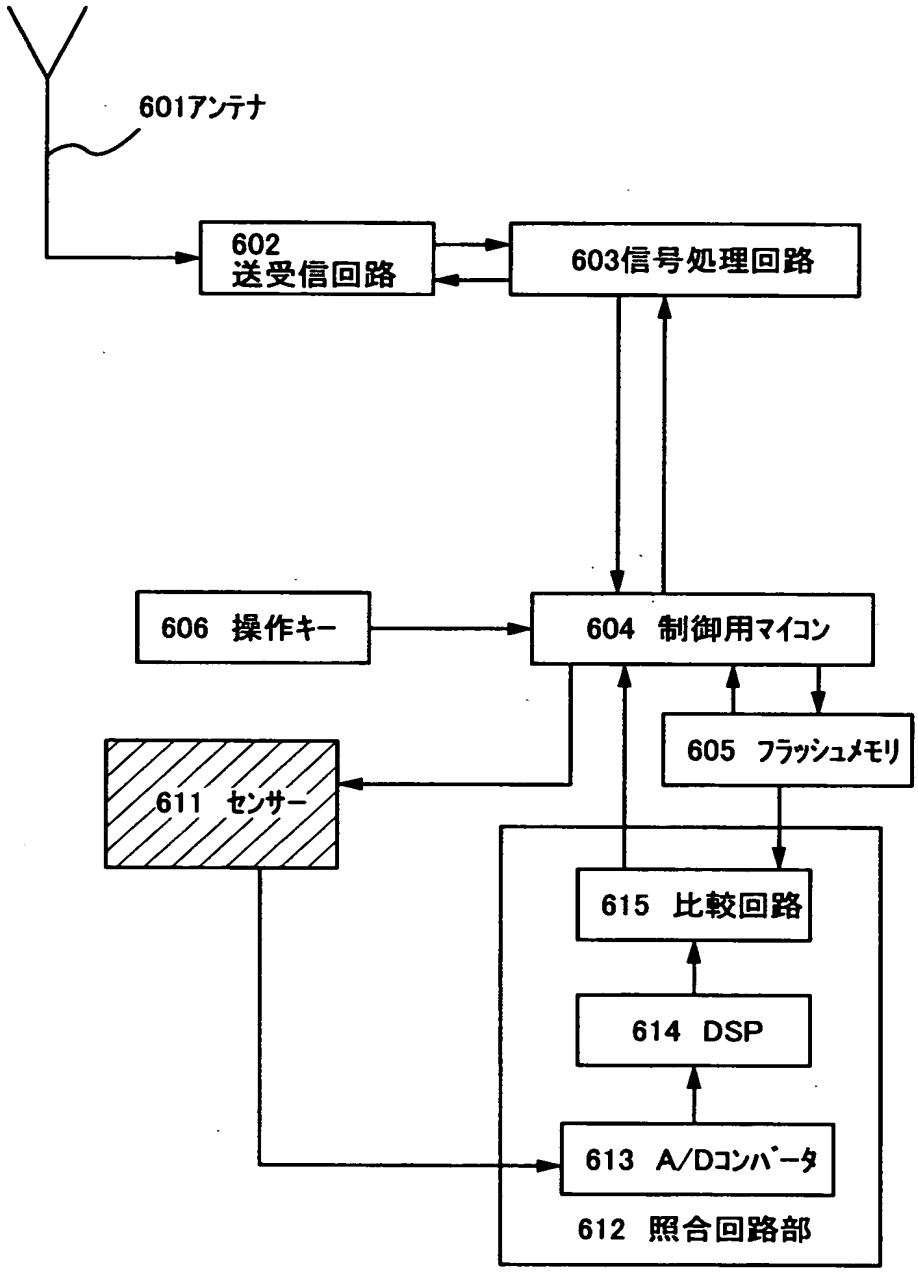


出証特２００１－３０１２５５６

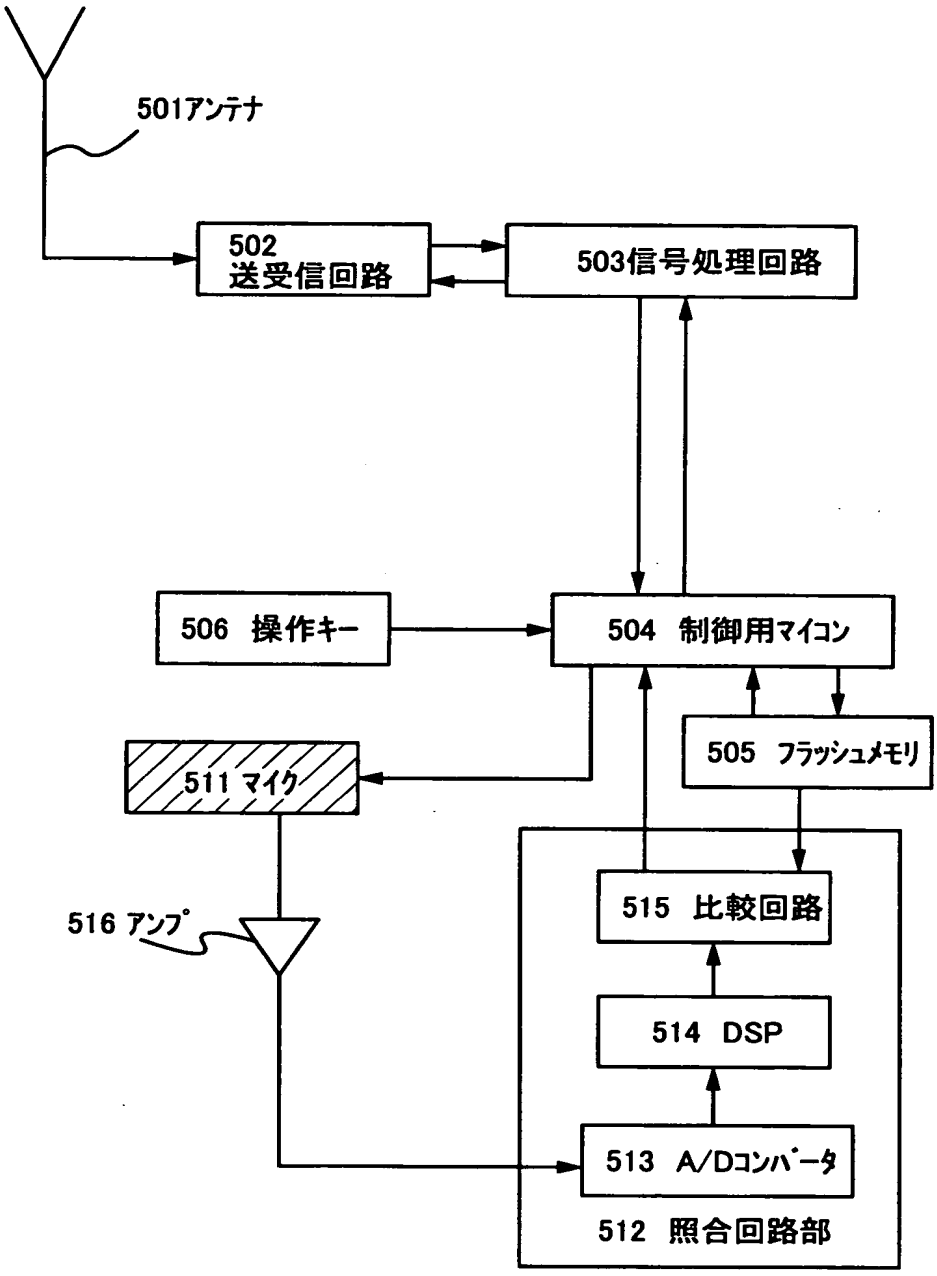
【図３】



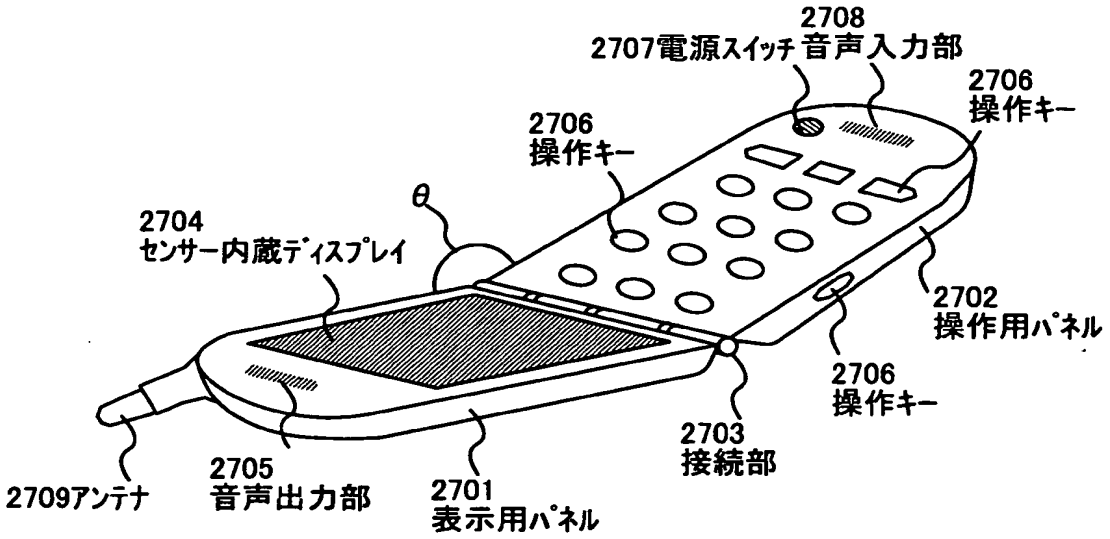
【図４】


601アンテナ
602
送受信回路
603信号処理回路
606 操作キー
604 制御用マイコン
605 フラッシュメモリ
611 センサー
615 比較回路
614 DSP
613 A/Dコンバータ
612 照合回路部

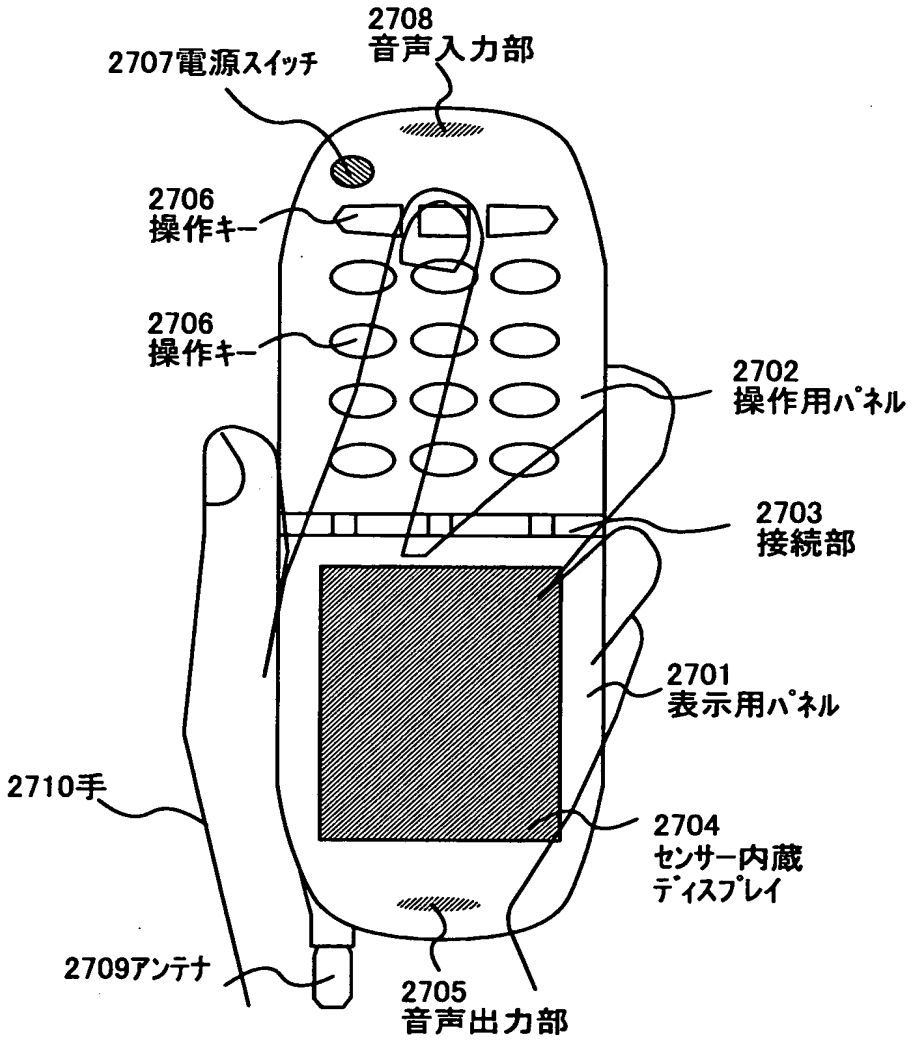
【図５】


501アンテナ
502
送受信回路
503信号処理回路
506 操作キー
504 制御用マイコン
505 フラッシュメモリ
511 マイク
516 アンプ
515 比較回路
514 DSP
513 A/Dコンバータ
512 照合回路部

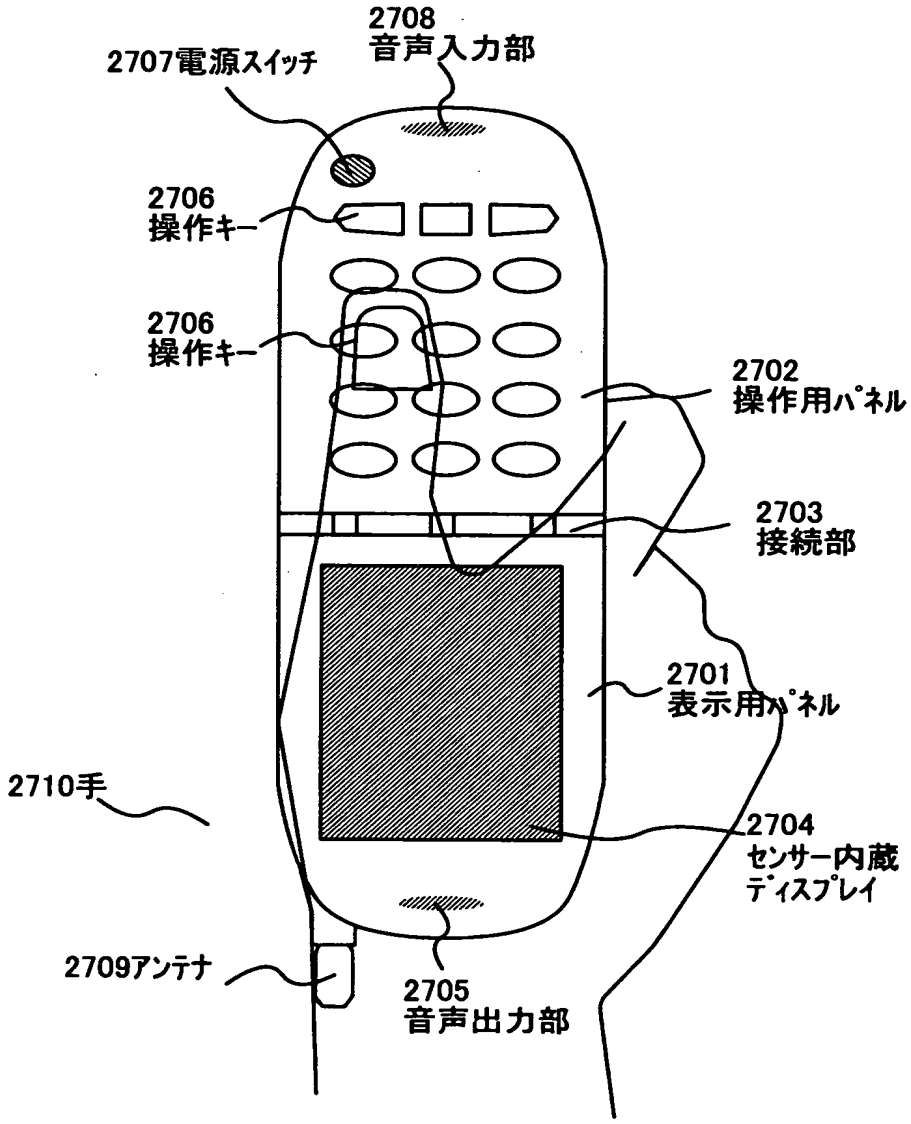
【図６】


2708
2707電源スイッチ
音声入力部
2706
操作キー
2706
操作キー
θ
2704
センサー内蔵ディスプレイ
2702
操作用パネル
2706
操作キー
2703
接続部
2709アンテナ
2705
音声出力部
2701
表示用パネル

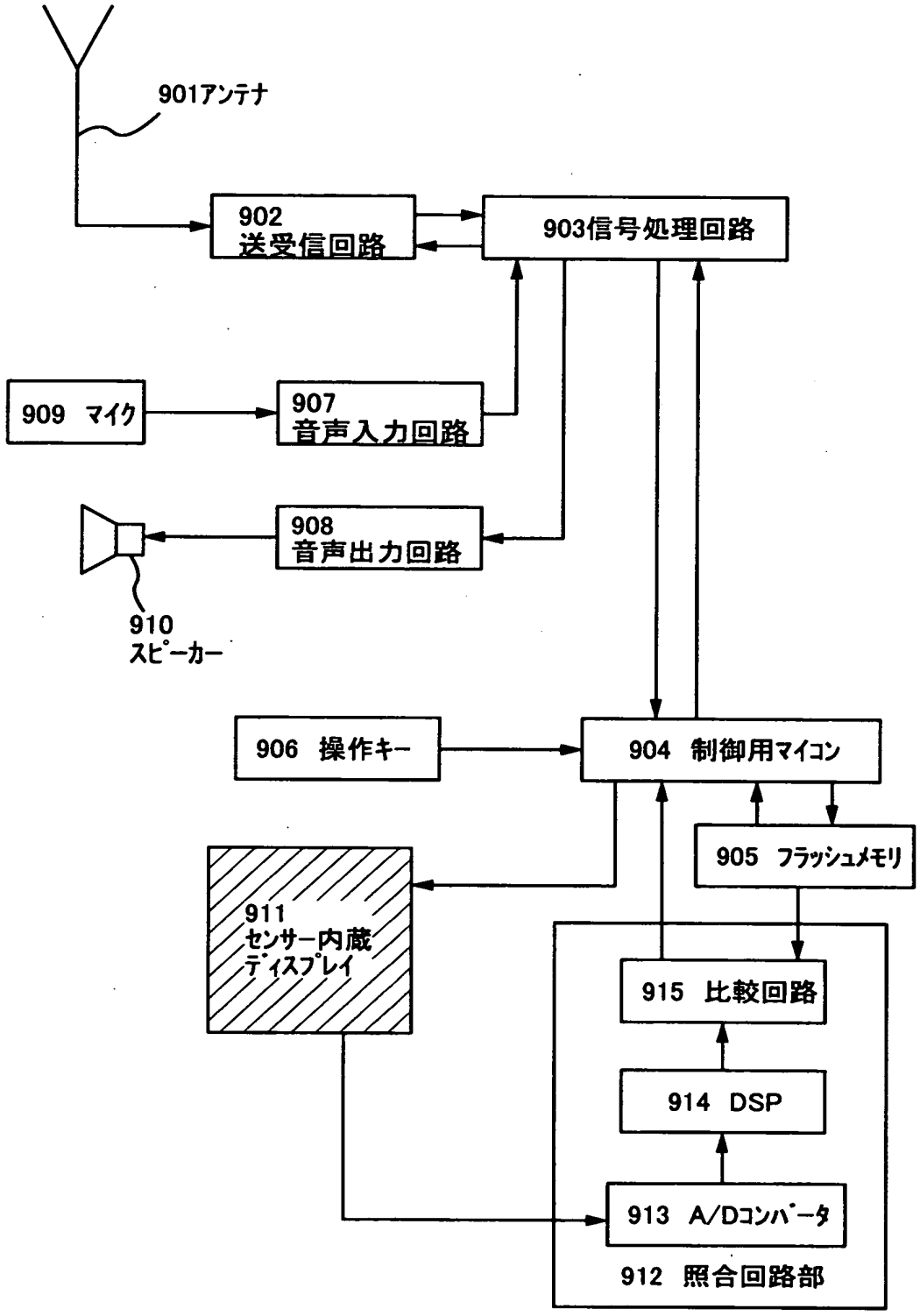
【図７】


2708
音声入力部
2707電源スイッチ
2706
操作キー
2706
操作キー
2702
操作用パネル
2703
接続部
2701
表示用パネル
2710手
2704
センサー内蔵
ディスプレイ
2709アンテナ
2705
音声出力部

【図８】

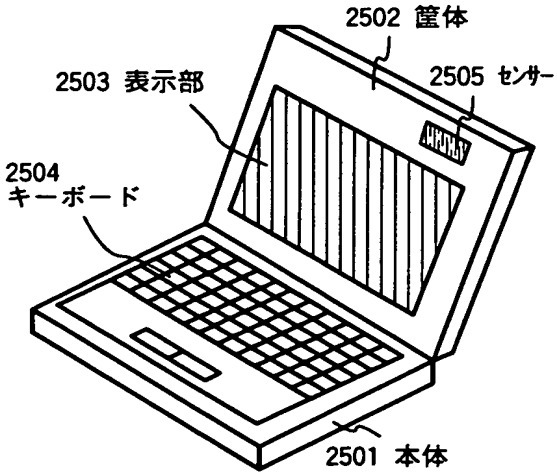

2708
音声入力部
2707電源スイッチ
2706
操作キー
2706
操作キー
2702
操作用パネル
2703
接続部
2701
表示用パネル
2710手
2704
センサー内蔵
ディスプレイ
2709アンテナ
2705
音声出力部

【図９】

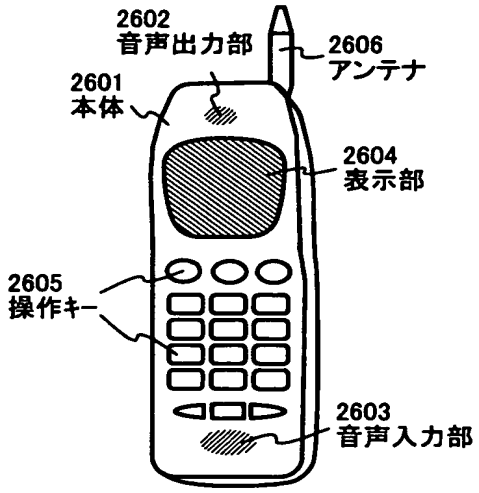

901アンテナ
902
送受信回路
903信号処理回路
909 マイク
907
音声入力回路
908
音声出力回路
910
スピーカー
906 操作キー
904 制御用マイコン
905 フラッシュメモリ
911
センサー内蔵
ディスプレイ
915 比較回路
914 DSP
913 A/Dコンバータ
912 照合回路部

【図１０】

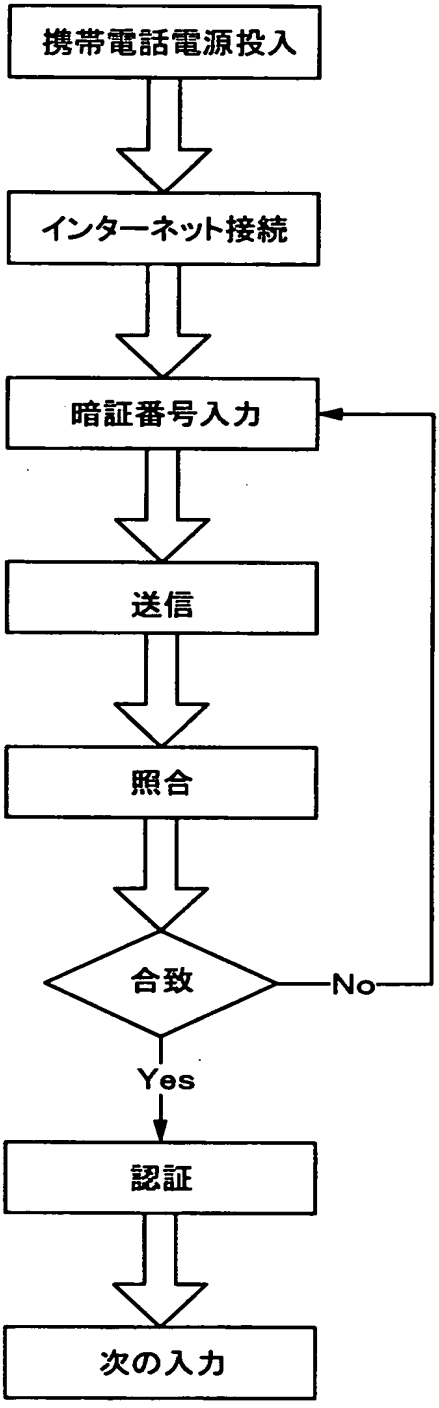
(A)


2502 筐体
2503 表示部
2505 ｾﾝｻｰ
2504
キーボード
2501 本体

(B)


2602
音声出力部
2606
アンテナ
2601
本体
2604
表示部
2605
操作キー
2603
音声入力部

【図１１】



【書類名】　要約書

【要約】

【課題】　顧客識別が容易な本人認証システムを提供する。

【解決手段】　顧客を識別する本人認証システムであって、前記顧客の生体情報を記憶する手段と、前記顧客の生体情報を読み取る手段と、前記読み取った生体情報を前記記憶した生体情報と照合する手段と、前記照合が合致した場合、サーバーに合致したことを情報として送る手段とを有することを特長とする本人認証システム。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔０００１５３８７８〕

１．変更年月日　　１９９０年　８月１７日
［変更理由］　新規登録
住　所　神奈川県厚木市長谷３９８番地
氏　名　株式会社半導体エネルギー研究所